
دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية

٥٨ ضابطاً عربياً يختتمون تدريباتهم بالأكاديمية على
مكافحة جرائم الحاسب الآلي



رئيس الأكاديمية في حفل الاختتام:
من أكبر الهواجس التي تواجه الدول كيفية الحفاظ على المعلومات التي تودع في الحاسوب

اختتم سعادة أ. د. عبدالعزيز بن صقر الغامدي رئيس أكاديمية نايف العربية للعلوم الأمنية صباح يوم العاشر من شهر ذي القعدة ١٤١٧هـ فعاليات الدورة التدريبية التي نظمها معهد التدريب بالأكاديمية وموضوعها (مكافحة جرائم الحاسب الآلي) وذلك بمشاركة ثمانية وخمسين ضابطاً من المملكة الأردنية الهاشمية والمملكة العربية السعودية وجمهورية السودان والجمهورية العربية السورية وسلطنة عمان ودولة الكويت والجماهيرية العربية الليبية الشعبية الاشتراكية العظمى.. وقد بدأ حفل الاختتام بتلاوة آيات من القرآن الكريم. ثم ألقى رئيس قسم البرامج التدريبية بمعهد التدريب كلمة استعرض فيها ما نفذه المعهد من دورات تدريبية في مجالات مكافحة الجريمة، ومنها جرائم الحاسب الآلي التي شارك فيها مئة وثلاثون متدرباً من الدول العربية.. بعد ذلك ألقيت كلمة المشاركين الذين أكدوا أن هذه الدورة أتاحت الفرصة لاكتساب العلم والخبرة وبناء أواصر الثقة والصداقة وتبادل الخبرات بين المشاركين من الدول العربية، وأضاف المشاركون بأن هذه الدورة مكنتهم من الإلمام بقضايا جرائم الحاسب الآلي ومدلولاتها الأمنية.

ثم ألقى سعادة رئيس الأكاديمية كلمة رحب فيها بالمشاركين، وأعرب عن سعادته بتخريج نخبة من الشباب العربي بعد أن تلقوا معلومات علمية في معالجة كثير من الجرائم في المجتمع، وهي جرائم لم تعد مقتصرة على الجريمة الميدانية بمطاردة المجرمين وإنما انتقلت إلى الآلة.

وأضاف سعادته أن بمقدار استفادتنا من هذه التجهيزات العلمية وبمقدار ما وصل العقل العلمي إلى تطوير هذه التجهيزات العلمية، فقد واصل الإجرام والمجرمون نقيض ذلك مستغلين هذه التجهيزات التي تفيد البشرية أسوأ استغلال. وأشار إلى أن من أكبر الهواجس التي تواجه الدول الكبرى، كيفية الحفاظ على المعلومات والأسرار العلمية التي تودع في الحاسوب، وهي أمور ينبغي أن يقوم عليها أناس لديهم الخبرة العلمية والاطلاع الواسع، وأن تعلم هذه المادة العلمية واستخدامها في التقنية يتطلب مواكبة المستجدات التي تساء في استخدام هذه الآلة. وقال رئيس الأكاديمية اننا قد حرصنا في هذه الدورة التدريبية على استقطاب نخبة ممن لهم باع طويل في هذا المجال، وفي مختلف الجوانب القانونية والاجتماعية والتطبيقية والعلمية المختلفة مستهدفين بذلك رفع كفاءة المتدربين وإلمامهم الكامل بهذه القضايا. وحث رئيس الأكاديمية الخريجين على يراعوا الله في الحفاظ على الأمانة، وقال: ندعو الله أن نكون عند حسن ظن أصحاب السمو والمعالي وزراء الداخلية العرب، وعند حسن ظن الرجل الأول الذي يقوم على هذه المؤسسة صاحب السمو الملكي الأمير نايف بن عبدالعزيز وزير الداخلية ورئيس مجلس إدارة أكاديمية نايف العربية للعلوم الأمنية الذي يوجهنا ويرشدنا دائماً إلى ما فيه الخير والصلاح للرفع من مستوى كفاءة رجل الأمن في وطننا العربي.. وفي الختام قام رئيس الأكاديمية بتسليم الشهادات للمتدربين.



المشاركون

هذه الدورة مكنتنا من الإلمام بقضايا جرائم الحاسب الآلي ومدلولاتها الأمنية .

فعاليات الدورة

هذا وكانت فعاليات مكافحة جرائم الحاسب الآلي قد بدأت صباح يوم الخامس عشر من شهر شوال ١٤١٧هـ واستمرت ثلاثة أسابيع قدم فيها أعضاء الهيئة العلمية موضوعات متعددة، وقد تولى مهمة الإشراف العلمي على هذه الدورة د.عبدالرحمن الشنيفي الذي قدم موضوعاً عن أمن المعلومات وجرائم الحاسب الآلي تناول فيه علاقة الحاسب الآلي بالجريمة، ولمحة تاريخية عن ميكنة الجريمة وطبيعة جرائم الحاسب الآلي.

وقد استهل د.الشنيفي موضوعه بإعادة الأذهان إلى حادث الطائرة النيوزيلندية من طراز دي سي ١٠ في شهر نوفمبر ١٩٧٩م عندما كانت متجهة إلى منطقة القطب الجنوبي وعلى متنها ١٢٧ راكباً حيث كانت الأمور تجري على ما يرام، وعند اقترابها من منطقة القطب أعطى المسئولون في القاعدة الأمريكية في ماكوردو الإذن بالهبوط دون مستوى السحاب وذلك من أجل أن يتمكن الركاب من الاستمتاع بالمناظر الموجودة في المنطقة ولكن بعد عدة دقائق اصطدمت الطائرة ببركان ثائر..

ويشير د. الشنيفي إلى أن التقارير الأولية دلت على أن الخطأ مصدره قائد الطائرة ولكن بعد إجراء كافة التحريات من قبل المسئولين اكتشف أن الحاسب الآلي في الطائرة قد تمت برمجته ليقود الطائرة للاصطدام مباشرة بالبركان الذي كان ارتفاعه ١٢ ألف قدم من سطح البحر.

لقد أصبح من المسلم به ـ كما يقول د. الشنيفي ـ أن جميع الدول لن تستطيع البقاء بعيداً عن استخدامات الحاسب الآلي من جهة، ولا عن ثورة تقنية المعلومات من جهة أخرى.

ميكنة الجريمة

وقدم د. الشنيفي لمحة تاريخية عن ميكنة الجريمة، فأوضح أن علاقة الحاسب الآلي بالجريمة ما هي إلاّ إفرازات الأنظمة الخاصة بأمن الحاسبات الآلية وذو طابع له خطورته وأهميته ، وأشار في هذا الصدد إلى أن الاحصاءات قد دلت على بلايين الدولارات قد سرقت من الكثير من المؤسسات المالية في الولايات المتحدة الأمريكية وحدها منذ عام ١٩٥٥م من خلال ألف قضية من قضايا ميكنة الجريمة، وهذا الرقم المالي المذهل يعكس الحالات التي يبلغ عنها من قبل هذه المؤسسات فقط، وهنا تكمن خطورة المشكلة لأنه لا أحد يعرف الرقم الحقيقي لعدد هذه القضايا لأن الكثير من المؤسسات والشركات الأخرى لم تبلغ عن السرقات التي تتم بهذا الأسلوب خشية رد الفعل السلبي الذي قد يؤثر على سمعة هذه المؤسسات والشركات ومكانتها المالية.

استبيان

وأشار د. الشنيفي إلى أن مجلة عالم الحاسب الآلي قامت بعمل استبيان في هذا الصدد لمئتي مؤسسة أمريكية واتضح أن (٣٣٠) من هذه المؤسسات اعترفت بأنها كانت ضحية لهذا النمط من الجريمة، وأن (٤٠) مؤسسة من هذه الـ (٦٠) ذكرت أن الذين قاموا بهذه الجرائم كانوا معروفين من قبل هذه المؤسسات وكانوا يعملون فيها كذلك أوضح الاستبيان أن تقديرات الخسائر المالية (اختلاس) قد وصلت ما بين ١٠ - ١٥ مليون دولار لكل عملية اختلاس وأنه لم يدن أي شخص متورط في هذه الاختلاسات. ويتابع د. الشنيفي القول.. ان كل جريمة لا تقع من فراغ، بل تقع دائماً نتيجة تفاعل مجموعتين من العوامل داخلية وخارجية مكتملة إلاّ إذا اتخذت هذه العوامل في الاعتبار، ومهما يكن من اهتمام الباحثين في بعض العوامل المسببة للسلوك الإجرامي دون الأخرى إلاّ أن لكل جريمة وضعها الخاص لأن كل فرد يختلف عن غيره في التكوين أو يختلف عن الآخر في الظروف البيئية المحيطة به.

وتحدث عن طبيعة جرائم الحاسب الآلي فأوضح أنها لا تعتبر نمطاً فريداً من نوعه يختلف عن بقية أنماط الجريمة بل إنه أصبح بإمكان المجرم أن يرتكب معظم أنواع الجرائم عن طريق الحاسب الآلي باستثناء جريمة القتل وما شابهها .

قضايا جرائم الحاسب الآلي

وقد لاحظ أن هناك مئات القضايا التي تتناول الدخول غير المصرح به لمئات الأنظمة الآلية المنتشرة في جميع أنحاء العالم، مشيراً إلى اختلاف الدوافع لهذه القضايا بحيث شملت الدخول لمجرد إشباع الرغبات الشخصية واللهو إلى قضايا ذات طابع أمني. وعند حديثه عن أمن الحاسب الآلي أشار د. الشنيفي إلى أن هذا المصطلح قد برز في السنوات القليلة الماضية ليأخذ مكان شد انتباه العديد من المهتمين بمجال الأمن خصوصاً أن أمن الحاسبات الآلية

. كل جريمة لا تقع من فراغ . . . ولكل جريمة وضعها الخاص لأن كل فرد يختلف عن غيره في التكوين والظروف البيئية المحيطة .

. هناك العديد من المستويات الأمنية التي يمكن أن تطبق على أنظمة الحاسبات الآلية .

والاتصالات في السابق كان الإجراء السائد يكمن في حماية الأجهزة فقط، هناك العديد من الأسباب التي تدعو إلى حماية منشآت الحاسب الآلي والتي منها على سبيل المثال:

- منع سرقة أو تدمير الأجهزة.
- منع سرقة أو تدمير البرامج.
- منع توقف الأجهزة والبرامج (النظام) وضمان استمراريته في الخدمة.

لذا فإن العديد من منشآت الحاسب الآلي تطبق الإجراءات اللازمة للحد من الوصول إلى غرف الأجهزة لغير المصرح لهم حتى أصبحت المقياس الوحيد للكثير من هذه المنشآت لحماية الحاسبات الآلية لديها... لكننا اليوم نعيش فيما يمكن تسميته بالجانب المظلم للتطور التقني اللامحدود.. فانتشار النهايات الطرفية في أماكن بعيدة من مقر النظام وتطور كل من الاتصالات وشبكات الاتصال جعل أمن الحاسبات الآلية مقصوراً على الأجهزة فقط بينما بقيت كل من المعلومات واستمرار النظام في


د. عبدالرحمن الشنيفي

. سهولة ارتكاب جرائم الحاسب الآلي والخسائر الفادحة التي تترتب عليها تعتبر من القوى الدافعة جداً من أجل وضع استراتيجية أمنية لمواجهة هذه الجرائم.

. هذه هي الإجراءات الواجب اتباعها حيال أمن الحاسبات الآلية.

الخدمة معرضين للكثير من الأخطار وتحت طائلة مجرمي الحاسب الآلي.

البناء الأمني

وتطرق للحديث عن البناء الأمني لنظام الحاسب الآلي فأشار إلى أن هناك العديد من المستويات الأمنية التي يمكن أن تطبق على أنظمة الحاسبات الآلية، ومن هذه المستويات مستوى يعالج أمن المنشآت والذي يستند على عدم السماح للأشخاص غير المصرح لهم بدخول مباني أجهزة الحاسب الآلي وأن أهم المكونات لهذا المستوى يعتمد على الأبواب المغلقة وحراسة مداخل ومخارج مباني الحاسب الآلي، ويمكن اعتبار هذا المستوى ذا أهمية أمنية كلية ليس كافياً لحماية الحاسب الآلي بشكل كامل. وهناك المستوى الثاني للبناء الأمني ويكمن في مستوى النظام، فالحاسبات الآلية الضخمة عادة ما تدار بأسلوب تدريجي لأنظمة البرامج، وإن أسلوب التدرج والسيطرة يعتمد على:

- برامج النظم التشغيلية تخاطب الحاسب الآلي مباشرة.
- برامج نظم قواعد المعلومات تخاطب النظم التشغيلية.
- برامج التشغيل وهي مراقبة النظام عامة والتي تستعمل للعديد من النشاطات والتي منها مراقبة الأشرطة والاتصالات وغيرها.
- البرامج التطبيقية تخاطب قواعد المعلومات أو شاشة مراقبة الأشرطة أو الاثنين معاً. وقال لقد جرت العادة أن يكون هناك الكثير من نشاطات النظام التي تحدث من خلال هذا التدرج والتي بالإمكان الحفاظ على أمن هذه النشاطات والمعلومات المتداولة من خلالها على جميع المستويات أو على بعضها حسب الطبقات الأمنية المستخدمة في النظام.

وخلص د. الشنيفي إلى القول بأن موضوع أمن الحاسبات الآلية والتخطيط الوقائي من أجل المواجهة الأمنية لجرائم الحاسب الآلي، في الكثير من المنشآت خصوصاً مراكز المعلومات موضوع مهمل ومنسي لدرجة كبيرة جداً، والسبب يعود إلى أن بعض المسئولين لا يجدون صعوبة في إقناع أنفسهم بأنه لن تحدث كارثة، لكن يمكن اعتبار هذه القناعة شيئاً جانبياً لأن المسئولية الأولى لهؤلاء المسئولين هي ضمان استمرارية تشغيل النظام فقط وليس في الحفاظ على مراكز المعلومات وما تحتويه من معلومات قد تكون ذات طابع سري هام، لذا فإن عدم النظر بجدية في هذا الشأن يعتبر تقصيراً كبيراً من قبل هؤلاء المسئولين في القيام بمسئولياتهم وتحملها بغض النظر عن وجهة نظرهم هذه. وأضاف بأن جرائم الحاسب الآلي قد تطورت خلال العقدين الماضيين معتمدة بذلك على التقدم التقني المذهل حتى أن الكثير من المجرمين بدأوا في متابعة هذه التقنية وذلك بحثاً عن وسائل جديدة لارتكاب جرائمهم، ومع أن هذه الفترة الزمنية كانت كافية من أجل الوصول إلى أفضل السبل والإجراءات لمواجهة هذه المشكلة إلاّ أن القليل من المهتمين بأمن الحاسبات الآلية والاتصالات قد لفت الانتباه إليها، لكن الوضع أخذ يتفاقم بدرجة عالية في السنوات القليلة الماضية بحيث أصبح من الضروري النظر إليه بجدية ذلك أن السرعة والدقة اللتين ترتكب بهما الجريمة قد استوليا على انتباه الجميع، لقد كانت ولا تزال السرقة بالطرق التقليدية تأخذ وقتاً قد يستغرق عدة ساعات لتنفيذها، لكن السرقة عن طريق الحاسب الآلي لا تتجاوز عدة ثوان لارتكابها، إضافة إلى أن باستطاعة المجرم مسح وإلغاء كافة الخطوات والسجلات

التي قد تدل على جريمته.

إن سهولة ارتكاب جرائم الحاسب الآلي والخسائر الفادحة التي تترتب عليها تعتبر من القوى الدافعة جداً من أجل وضع استراتيجية أمنية فعالة لمواجهة هذه الجرائم وأن صعوبة إثبات عناصر الجريمة في الكثير من الحالات ضمن التشريعات والقوانين الجنائية التقليدية أدي إلى ضرورة تشريع قوانين محددة لنشاطات الحاسب الآلي، هذا بالإضافة إلى صعوبة فهم مبادئ الحاسب الآلي مما أدى إلى صعوبة إصدار حكم في الكثير من القضايا من قبل القضاء والمشرعين. وتناول د. الشنيفي عدداً من الإجراءات الواجب اتباعها حيال أمن الحاسبات الآلية ومنها:

- الطلب من المنشأة التي لديها الرغبة في إدخال الحاسب الآلي بوضع تصور أمني واضح المعالم جلي الأهداف مبرزاً جميع الجوانب المراد تطبيق وسائل أو إجراءات الأمن والحماية عليها بدقة والمتمثلة بأمن المنشآت والعاملين والبرامج وشبكة الاتصالات.
- يلزم إجراء دراسة مسح شامل لجميع مكونات النظام من فنيين وأجهزة وبرامج ووثائق بصفة دورية وتحديد مناطق الضعف ومن ثم تصحيحها.
- عدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية.
- يجب تبني خطة استراتيجية بعيدة المدى لتأهيل الكوادر الوطنية الفنية والحفاظ على هذه الكوادر من التسرب وتقديم كافة الدعم المالي والمعنوي للعناصر المهمة العاملة على النظام، وتنويع مصادر الأجهزة والبرامج من أجل كسر عامل الاحتكار من قبل كثير من الشركات.

جرائم الحاسب الآلي الدولية

وفي موضوع آخر عن جرائم الحاسب الآلي الدولية تناول د. ذياب البداينة بلغة الأرقام كلفة جرائم الحاسب الآلي في عدد من دول العالم من بينها الولايات المتحدة الأمريكية والمنطقة العربية وأشار إلى أن استخدام الحاسب قد أصبح سمة من سمات العصر، وغدا العالم قرية كونية بفعل الربط الإلكتروني (الإنترنت) وغيره. وأصبح الفرد قادراً على التسوق، والبحث عن المعلومات ونقلها، والتواصل مع الثقافات الأخرى بسهولة ويسر من خلال الحاسب وتوابعه من المعدات الأخرى، وكأي نوع آخر من التقنيات، فإن استخدام الحاسب قد قدم للإنسان وظائف إيجابية جبارة في كافة المجالات الحياتية، إلاّ أنه قد واكب هذا الاستخدام نتائج سلبية كذلك أهمها جرائم الحاسب، وأوضح أن هذا النوع من الجرائم قد أصبح بلا حدود، حيث يمكن أن يكون المجرم في مكان ما ويقوم بجريمته في مكان آخر. وأضاف بأن جرائم الحاسب ظاهرة عالمية وأن التحقيق فيها والحكم عليها عملية معقدة، وتعد هذه الجرائم مثلها مثل جرائم أصحاب الياقات البيضاءمن الجرائم التي يصعب التنبؤ بها، ومن الصعب محاكمة منفذيها، وذلك لعدم توافر أدلة مادية فيها، أو شهود، ولأن تقنيات الحاسب في تطور كبير فلم يواكب هذا التطور تعريفات واضحة ومحددة وتشريعات قانونية مناسبة لها.

استخدام الحاسب قدم للإنسان وظائف إيجابية جبارة في كافة المجالات

جرائم الحاسب الآلي ظاهرة عالمية والتحقيق فيها عملية معقدة

ولاحظ د. البداينة أن جرائم الحاسب ترتكب من قبل الأفراد أكثر مما ترتكب من قبل محترفي الحاسب، كما يمكن أن ترتكب من مديرين يبحثون عن الثراء أو السلطة، أو من قبل مؤسسات تبحث عن معلومات عن منافسيها، أو من وسائل إعلام تبحث عن معلومات أو أخبار أو من قبل حكومات تبحث عن معلومات تجارية، أو جريمة منظمة تبحث عن ملفات موثوقة. وأضاف بأن المجرم عندما يستخدم الحاسب كأداة للجريمة فإن الجرائم المرتكبة عادة ما تكون جرائم تقليدية مثل الاحتيال المالي، السرقة، ويتم استخدام الحاسب هنا كوسيلة للجريمة وتقع غالبية جرائم الحاسب الأمريكية في هذه الفئة. وعند حديثه عن الحاسب كهدف للجريمة أوضح أن ذلك نوع جديد من أنواع الجريمة تطور بفعل تطور الحاسبات، حيث يمكن أن تستهدف الجريمة الحاسب بمعداته الفيزيقية وتوابعه من هذه المعدات، والبرمجيات، والبيانات، والمعلومات المخزنة فيه، وقد يكون الجناة في هذا النوع من الداخل (موظفين) أو من



الدكتور ذياب البداينة

استخدام الانترنت يعد من الاستخدامات الداعمة للأجهزة الأمنية.

الإنترنت من أهم الوسائل التي ساهمت في تكوين ثقافة عالمية من خلال إمكانية التواصل بين الأفراد.

الخارج (مجرمين)، وغالباً ما يستخدم الدخول الخارجي غير القانوني (غير الشرعي) وسائل اتصال تمكن من الوصول إلى أنظمة الحاسوب.

وأضاف د. البداينة أن جرائم الحاسوب لن تكون مقتصرة على دولة ما بعينها، وإنما سيكون العالم كله مسرحاً لها، حيث يمكن للفرد أن يرتكب جريمة من أي مكان في العالم وفي أي مكان فلا وجود للحدود العالمية في جرائم الحاسب خاصة مع وجود الإنترنت، وشبكات الاتصال العالمية، وتزداد الخطورة من أن قادة الجريمة يمكنهم من توظيف طاقات إبداعية في هذه المجالات وتحت نشاطات مقبولة اجتماعياً ولكن بقصد توظيف واستثمار أموال الجريمة عامة وتطوير قدراتهم التقنية الجرمية.

الإنترنت

وفي حديثه عن الإنترنت أوضح د. البداينة أنها تمثل تواجداً عالمياً دون قيود فالكل يعرض ما لديه والكل يتسوق في عالم من الثقافات المتعددة، إن ما يميز عصر المعلومات هو توافرها وسهولة الحصول عليها، وفي أحيان كثيرة تبحث المعلومات عن العملاء لها. وقال ان الفائدة المتحققة أو الخسارة الناجمة عن الدخول إلى العالم الإلكتروني تتحدد بأهداف المستخدم، إن ما يبحث عنه المستخدم هو المعيار في الحكم على الفائدة أوالضرر. وفي هذا المجال فإن المعيار المستخدم كإطار مرجعي للحكم إنما هو معيار اجتماعي وليس موضوعياً. وبالتالي فإن الحكم على الفائدة أو الخسارة يتحدد بالاجماع الاجتماعي، وبما يسود من قيم وثقافات أو شخصيات المستخدمين، وبالتالي يصعب تطبيق معيار الصح أو الخطأ.

وأشار د. البداينة إلى أن الإنترنت تعد من أهم الوسائل التقنية التي ساهمت في تكوين ثقافة عالمية من خلال إمكانية التواصل العالمي بين الأفراد، والفرص المتاحة للتعرف على الثقافات الاجتماعية الأخرى، إن توافر المعلومات بشكل كبير وإمكانية استرجاعها بفترة زمنية قصيرة، والاطلاع عليها جعل إمكانات الفهم الثقافي العالمي أكبر من أي وقت سبق، وأن امتياز شبكات الانترنت بإمكانية التواصل ليس المكتوب فقط، وإنما المشاهد، والمسموع، والفاعل قد مكن من التواصل والتقارب المكاني بين الأفراد رغم اختلاف الزمن والمكان والثقافة ويدعم هذا نظام الشبكة الذي أصبح يحمل إمكانية الترجمة والكتابة بلغات متعددة.

وفي جانب آخر من محاضرته تحدث د. البداينة عن النشاط



الاقتصادي عبر الإنترنت فأشار إلى أن البنوك تخسر مبالغ كبيرة قدرت في بريطانيا ب ٢,٧ بليون باوند سنوياً نتيجة الاحتيال المالي وسوء الاستخدام لبطاقات التسليف،وهذه من الطرق التقليدية في التعامل المالي، إن المؤسسات المالية ضحية للاحتيال المالي ليس بسبب الإنترنت، ففي بداية ١٩٩٥م أظهرت نتائج دراسة ماستر كارد المسحية أن ٦٦٪ من المستجيبين قد استخدموا الـ Web للاطلاع على البضائع وأن ٢٨٪ منهم قد اشترى عن طريقها، في حين رأي ٨٥٪ منهم أن الإنترنت قناة مهمة للاطلاع والاختيار من المواد المعروضة والخلاصة هي أن الأفراد قد قبلوا الإنترنت كمكان آمن.

المنظور الأمني

وأضاف د. البداينة أن استخدام الإنترنت يعد من الاستخدامات الداعمة للأجهزة الأمنية ففي مجال شرطة المجتمع يمكن استخدام الإنترنت في تعقب المجرمين وفي التواصل السريع مع الشرطة لكشف الجريمة.

كذلك يمكن استخدام الإنترنت في إرسال الرسائل الأمنية للعاملين في القطاع الأمني بشكل دوري، ومنظم وسريع، فلا حاجة لإعادة كتابة الرسائل، فيكفي كتابة رسالة مرة واحدة تمكن من إرسالها إلى عدد كبير من العملاء أو الزبائن، كما يمكن أن تستخدم الإنترنت في تقديم خدمات سريعة للجمهور، وفي تعميق الوعي الأمني لديهم من خلال عمل صفحات خاصة بالشرطة تحوي إرشادات أمنية عامة، وقد تنشر صور المطلوبين للعدالة أو الأشخاص الخطرين على أمن المجتمع والطلب من الجمهور التعرف عليهم وتسليمهم للعدالة.

إجراءات المواجهة

وتطرق البداينة إلى إجراءات مواجهة جرائم الحاسب على المستويين الوطني والعالمي فعلى المستوى الوطن أشار إلي أن خبراء الأمن المعلوماتي وصانعي السياسات الحكومية ومسوقي الحاسب والأفراد المهتمين في هذا الموضوع بحاجة إلى تغيير نظرتهم تجاه جرائم الحاسب، لا لأنها مشكلة وطنية فقط، وإنما كمشكلة عالمية وتتطلب الإجراءات الوطنية تعاوناً في مجال القطاعين العام والخاص، فعلى القطاع الخاص الالتزام بإجراءات الوقاية، وعلى القطاع العام تنفيذ الإجراءات اللازمة لمكافحة المشكلة، وبشكل عام هناك حاجة لوجود التشريعات اللازمة لحماية ملكية الحاسب، والبيانات، والمعلومات والمعدات اللازمة للتشغيل والتوصيل، والوعي الوطني لجرائم الحاسب والعقوبات المترتبة عليها.

ووجود المؤسسات المختصة في التحقيق في جرائم الحاسب (في المحكمة ولدى الشرطة).

والتعاون مع الدول الأخرى في الحماية والوقاية من هذه الجرائم.

. جرائم الكمبيوتر تعتبر شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو القارية.

. نظم الكمبيوتر تتيح بعض الفرص لصور جديدة من الجرائم لم تكن موجودة في الماضي.

. الضرورة تقتضي تجريم الأنشطة الخاصة بإساءة استخدام الكمبيوتر واتخاذ الإجراءات اللازمة لتأمينه.

. إساءة الاستعمال المتكرر تؤدي إلى زيادة حجم إجرام نظم المعلومات.

وعلى المستوى العالمي يجب الاهتمام بمشكلة جرائم الحاسب وخصوصاً في مجال التشريعات والتعاون والتبادل، ويرى مركز الأمم المتحدة للتطوير الاجتماعي والشئون الانسانية أن الوقاية من جرائم الحاسب تعتمد على الأمن في إجراءات معالجة المعلومات، والبيانات الالكترونية ، وتعاون ضحايا جرائم الحاسب، ومنفذي القانون، والتدريب القانوني، وتطور



د. محمد محيي الدين عوض

القانوني لجرائم الحاسب والإجراءات القانونية لمكافحتها، ولاحظ أن النواحي المشرقة للكمبيوتر وتقنية المعلومات يقابلها من الناحية الأخرى جوانب سلبية لأنها تجعل الباب مفتوحا على مصراعيه لأنواع من السلوك المنحرف اجتماعياً التي لم يكن من الممكن تصور وقوعها في الماضي وبالتالي ليست مجرمة في كثير من الدول.

فنظم الكمبيوتر تتيح بعض الفرص لصور جديدة من الجرائم لم

وإفساد المعلومات المخزنة في قواعد الكمبيوتر. وقال إن سرعة انتشار شبكات الكمبيوتر عبر الحدود والتغير التقني المطرد والمتعاظم في هذا المجال وإمكان اختراق كثير من نظم المعلومات عن طريق خطوط الهاتف العادي أو عن طريق إجبار أو إغراء العاملين عليها والحصول على كلمة السر، وبالتالي التداخل فيها زاد من فرص إساءة استخدام الكمبيوتر كوسيلة تقنية أو ارتكاب تغيير في البرامج أو المعلومات المخزنة فيه وذلك في غياب القوانين الجنائية الموضوعية ونظم العدالة الجنائية المواكبة لهذه الطفرة، وكذلك في غياب التعاون والتضامن الدولي لمواجهة هذه الأنواع من السلوك الجديد المنحرف علماً بأنه ليس هناك دول قليلة لديها قوانين ملائمة لمواجهة هذه المشكلة.



أخلاقيات استخدام الحاسب، والأمن الدولي لأنظمة المعلومات. ففي المجال الدولي هناك حاجة للتعاون الدولي المتبادل.

مشكلات الجرائم المتعلقة بإساءة استخدام الكمبيوتر

ومن الموضوعات التي تابعتها مجلة الأمن والحياة موضوع قدمه د.محمد محيي الدين عوض تناول فيه النواحي القانونية لأمن الحاسب الآلي والتوصيف

تكن موجودة في الماضي كما أنها تتيح الفرصة لارتكاب الجرائم التقليدية بطرق غير تقليدية. أما الصور الجديدة فمن أمثلتها سرقة المعلومات والأسرار المودعة في قواعد المعلومات لأن الحصول على المعلومات دون رضا أو الإضرار بها ليس هو الصورة المألوفة للسرقة التي تقع على الأموال الحسية المادية. وأما الجرائم التقليدية التي ترتكب بطرق غير تقليدية فمن أمثلتها الغش والتزوير وإتلاف

لا تعترف بالحدود

وأضاف د. محمد محيي الدين عوض أن جريمة الكمبيوتر لا تعترف بالحدود بين الدول والقارات إذ يكفي أن نتصور أن القائم على الكمبيوتر في طوكيو يستطيع أن يحول مبلغاً من المال من هناك إلى نيويورك أو مونتريال مضيفاً إليه صفراً أو بضعة أصفار في مونتريال بكندا أو نيويورك في الولايات المتحدة الأمريكية، كذلك يستطيع من لديه إحدى النهايات ويعرف كلمة السر أن يفعل الأمر نفسه بتغيير المعلومات في جميع الشبكة الأوربية

التي يتصل بها من أقصى الشرق عن طريق التداخل فيها.

فجريمة الكمبيوتر تعتبر شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية، ولمواجهة مثل هذه الجريمة مواجهة فعالة يجب:

أولاً : تجريم صورها في القانون الوطني للمعاقبة عليها إذا لم يكن هناك نص يواجهها.

ثانياً: أن يكون هناك تعاوناً وتضامناً دولياً لمواجهة مشكلاتها من حيث مكان وقوعها واختصاص المحاكم بها، وجمع المعلومات والتحريات عنها، والتنسيق بين الدول في المعاقبة عليها وتنفيذ الأحكام الصادرة بصددها، وتحديد صورها وإيجاد الحلول لهذه المشكلات والاتفاق على قواعد التسلم فيها .. إلى غير ذلك.

وقد استعرض د. عوض بعض المشكلات المتعلقة بالتعاون الدولي حول جريمة الكمبيوتر مشيراً إلى أن هذه المشكلات قد تمت معالجتها إلى حد كبير في قوانين قليلة في العالم كما أنها عولجت إلى حد ما أيضاً على المستويين الدولي أو الإقليمي وخصوصاً في منظمة التعاون والإنماء الاقتصادي الأوربية ومجلس أوربا ووضعت هذه الجهات خطوطاً إرشادية للمشرعين وراسمي السياسات الجنائية في دولها.

وقد أكد د. محمد محيي الدين عوض أن الضرورة تقتضي تجريم الأنشطة الخاصة بإساءة استخدام الكمبيوتر واتخاذ التدابير اللازمة لتأمينه والوقاية من إساءة استخدامه آخذين في الاعتبار الصعوبات المتعلقة بحماية حقوق الإنسان في حياته الخاصة وغيرها من الحقوق والحريات العامة غير غافلين عن حماية التجارة الدولية والمصالح الاقتصادية والأنشطة المالية حماية فعالة وكفالة حرية الاتصال وتبادل المعلومات والبيانات والخبرات دون إعاقة لعمليات الكمبيوتر من ناحية أخرى سواء كانت تلك العمليات متعلقة بالمال والبنوك أو الاقتصاد أو الخدمات العامة أو الخاصة.

كما يجب من ناحية أخرى تلافي العيوب المتعلقة بالإجراءات سواء من



ناحية التحري أو التحقيق أو المحاكمة أو الإثبات وتدريب القائمين عليها على كيفية النجاح في الاتهام والإدانة حتى يتحقق المنع. وقال إن القوانين الموضوعية والإجرائية يجب تعديلها بما يتفق ومكافحة منع هذا النوع الجديد من الانحراف والإجرام وذلك لأن القوانين الخاصة بالإجرام التقليدي غير ملائمة. كما يجب أن يكون هناك تعاون دولي في سبيل مكافحة هذه الجرائم وتبادل المعلومات عنها وعن مرتكبيها ليتسنى كشفها وإثباتها والإدانة فيها.

وكذلك الوقوف على كيفية معالجة الدول الأخرى لهذا النوع الجديد من الجرائم من الناحيتين الموضوعية والإجرائية. ويدخل في التعاون الدولي أيضاً المساعدة في تسليم المجرمين وجمع الأدلة وتنفيذ الأحكام الأجنبية والإنابات القضائية للحصول على ما يساعد على الاتهام.

ثلاثة أمور

وقد أرجع د. محيي الدين عوض إجرام نظم المعلومات إلى ثلاثة أمور:

١ ـ التلاعب في الحاسب الآلي وما يحويه من معلومات وبأدواته.

٢ ـ التجسس عليه.

٣ ـ الاستخدام غير المشروع له.

وقد يتضمن هذا الإجرام انتهاكاً لحق الإنسان في حياته الخاصة مثل الحصول على معلومات عن مريض في مستشفي أو التلاعب بنوافذ الصرف الآلي في البنوك أو سرقة برامج الحاسب الآلي ويعطى علماء الإجرام أهمية لأمرين:

ـ برامج الفيروس.

ـ التلاعب في التحويل الالكتروني للأموال.

وقد اهتم الرأي العام بالفيروس عام ١٩٨٩م عندما ظهر في إحدى القضايا الجنائية بألمانيا أن الفيروس قد نفذ عن طريق شبكة معلومات دولية إلى أنظمة المعلومات الأمريكية والإنجليزية والبلاد الأوربية الأخري، وقد بيع المتحصل عليه من المعلومات للجهات السوفييتية KGB وفي سنة ١٩٨٨م أصبحت أخطار برامج الفيروس واضحة وأن طالباً أمريكياً نجح في تعطيل ٦٠٠٠ حاسب لعدة أيام. وأضاف بأن إساءة الاستعمال المتكرر سوف تؤدي إلى زيادة حجم إجرام نظم المعلومات خصوصاً وأن الاقتصاد والإدارة والمجتمع ككل يعتمد في جانب كبير منه على الأمن الفعال لنظم المعلومات. مع ملاحظة أن أغلبية التحويلات النقدية تتم الآن عن طريق الحاسبات، وفي كثير من المؤسسات يعتمد كل الإنتاج على العقل الإلكتروني، وتقوم كثير من الشركات بتخزين أسرار صفقاتها الهامة بالحاسب، والإدارة العامة تعمل بنظم المعلومات وكذلك يتم عن طريقها مراقبة التهريب البحري والمراقبة الطبية أيضاً تتم على أساس التكنيك المعلوماتي ويلاحظ أن التشريع الجنائي وحده ليس كافياً وإنما يجب أن تتخذ إلي جانب التشريع الجنائي إجراءات غير تشريعية للتأمين ضد هذا النوع من الإجرام.

أمن المعلومات

ومن الموضوعات التي قدمت في الدورة موضوع للمهندس حسن طاهر داود تحدث فيه عن أمن المعلومات وذلك بالتركيز على الجوانب الفنية والإدارية للوقاية من جرائم الحاسب الآلي وتحدث عن الفيروس الذي قال بأنه في حقيقته برنامج من برامج الحاسب ولكن تم تصميمه بهدف إلحاق الضرر بنظام الحاسب وحتى يتحقق ذلك يلزم أن تكون لهذا البرنامج القدرة على ربط نفسه بالبرامج الأخرى وكذلك القدرة على إعادة تكرار نفسه بحيث يتوالد ويتكاثر مما يتيح له فرصة الانتشار داخل جهاز الحاسب في أكثر من مكان في الذاكرة ليدمر البرامج والبيانات الموجودة في ذاكرة الجهاز.

وتكمن خطورة الفيروس في أنه مثل الفيروس الذي يصيب الجسم الإنساني قادر على الانتقال من جهاز إلى آخر بسرعة كبيرة والسبب في ذلك التقدم الكبير الذي وصلت إليه وسائل الاتصال وشبكات الحاسب مما أدى إلى سهولة الاتصال بين أجهزة الحاسب وبعضها والتي ربما تكون في قارات متباعدة، كما أدى توافق نظم التشغيل واتباعها للمعايير إلى زيادة انتشار الفيروسات حيث يستطيع البرنامج الواحد الآن أن يعمل على أنواع مختلفة من الحاسبات ونسخ مختلفة من نظام التشغيل، والعامل الثالث الذي أدى إلي زيادة انتشار

الفيروسات هو قرصنة البرامج التي جعلت نسخ البرامج غير الأصلية موضع التداول بين الكثير من الأجهزة، مما أوجد ثغرة كبيرة تنفذ من خلالها البرامج الملوثة بالفيروسات.

وتطرق إلى أنواع الفيروسات فأوضح أنها تأخذ أشكالاً عديدة فقد تشبه الدودة في توالدها وتكاثرها، وقد يتم إدخالها إلي النظام لتحدث التخريب المطلوب في توقيت معين أو عند حدوث واقعة معينة. واستعرض المهندس داود بعض أشكال الفيروسات ومنها:

ـ حصان طروادة Trogan Hourse: وهو جزء صغير من الكود يضاف إلى البرمجيات ولا يخدم الوظائف العادية التي صممت من أجلها هذه البرمجيات ولكنه يؤدي عملاً تخريبياً للنظام وتكمن خطورته في أن النظام لا يشعر بوجوده حتى تحين اللحظة المحددة ليؤدي دوره التخريبي.

ـ القنابل المنطقية Logic Bombs: القنبلة المنطقية هي أحد أنواع حصان طروادة وتصمم بحيث تعمل عند حدوث ظروف معينة أو لدى تنفيذ أمر معين، فقد تصمم بحي تثعمل عند بلوغ عدد الموظفين في الشركة عدداً معيناً من الموظفين مثلاً أو إذا تم رفع اسم المخرب (واضع القنبلة) من كشوف الرواتب. وتؤدي القنبلة في هذه الحالة إلى تخريب بعض النظم أو إلي مسح بعض البيانات أو تعطيل النظام عن العمل.

ـ القنابل الموقوتة Time Bombs: القنبلة الموقوتة هي نوع خاص من القنابل المنطقية وهي تعمل في ساعة محددة في يوم معين كأن تحدث مثلاً عندما يوافق اليوم الثالث عشر من الشهر يوم جمعة.

ـ باب المصيدة Trabdoor: هذا الكود يوضع عمداً بحيث يتم لدى حدوث ظرف معين تجاوز نظم الحماية والأمن في النظام. ويتم زرع هذا الكود عند تركيب النظام بحيث يعطي المخرب حرية تحديد الوقت الذي يشاء لتخريب النظام فهو يظل غير مؤذ حتى يقرر المخرب استخدامه، وكمثال على ذلك إقحام كود في نظام الحماية والأمن يتعرف على شخصية المخرب ويفتح له الأبواب دون إجراء الفحوص المعتادة.

ـ الديدان Worms: الدودة هي عبارة عن كود يسبب أذى للنظام عند استدعائه، وتتميز الدودة بقدرتها على إعادة توليد نفسها، بمعنى أن أي ملف أو جهاز متصل بالشبكة تصل إليه الدودة يتلوث. وتنتقل هذه الدودة إلى ملف آخر أو جهاز آخر في الشبكة. وهكذا تنتشر الدودة وتتوالد.

طرق الوقاية من الفيروسات

وأشار المهندس داود إلي أن هناك عدة إجراءات وقائية يعفي تطبيقها المؤسسة من كثير من العواقب الوخيمة التي قد تترتب على الإصابة بالفيروسات مثل:

ـ تجهيز عدة نسخ من البرمجيات وحفظها بحيث يمكن استرجاع نسخة نظيفة (غير ملوثة بالفيروس) من البرنامج عند الحاجة.

ـ الاحتفاظ بسجل لكل عمليات التعديل في برامج التطبيقات بحيث يتم تسجيل جميع وقائع نقل البرامج المعدلة إلى البيئة الإنتاجية، وخصوصاً تلك البرامج المجلوبة من خاج المؤسسة.

ـ يجب توعية المستخدمين بعدم تحميل أي برنامج مجلوب من الخارج في حاسباتهم الشخصية، فهذا هو أوسع الأبواب لإدخال فيروسات إلى النظم والتي عند دخولها ربما تصيب جميع الأقراص وجميع الأجهزة بالشبكة، والبرامج المجانية التي تنتقل من يد إلى يد أو يتم توزيعها بواسطة مجلات الكمبيوتر المتخصصة يجب دائماً الحذر في التعامل معها. حتى تلك البرامج التي تأتي من مصادر لا يرقى إليها الشك يجب فحصها جيداً.

ـ عند فحص البرمجيات أو اختبارها قبل السماح بنشرها في المؤسسة للاستخدام العام يجب أن يتم ذلك على جهاز مستقل غير مرتبط بالشبكة، ويجب أن يتضمن الاختبار عن أي سلوك غير مفهوم في البرنامج كأن يخرج رسائل لا داعي لها على الشاشة مثلاً ولو أن خلو البرنامج من مثل هذا السلوك غير المفهو لا يعني بالضرورة نظافة البرنامج فالفيروسات تظل كامنة ولا تكشف عن سلوكها إلاّ في اللحظة المناسبة.

ـ تركيب برنامج للتحقق من وجود



المهندس حسن داود

فيروسات ويفضل أن يكون هذا البرنامج دائم الوجود في الذاكرة، وهذه البرامج تقوم بالتأكد من عدم وجود الفيروسات المعروفة لها، ولذلك فهي تكون عديمة الفائدة في مواجهة الفيروسات الجديدة، وبعض هذه البرامج يقوم بمقارنة محتويات بعض مناطق القرص (الصلب أو اللين) أو بعض مناطق الذاكرة بمحتوياتها المتوقعة والمفترض أن توجد بها والإبلاغ عن أي تغير فيها مما قد ينبئ عن وجود فيروس.

ويجب عدم إجازة البرامج للاستخدام العام في المؤسسة إلاّ بعد اجتيازها بنجاح هذه الاختبارات.

نصائح

ويقدم المهندس حسن داود عدداً من النصائح للمستخدم من أجل تأمين الحاسب الشخصي ، ومن هذه النصائح:

- الاحتفاظ بنسخ احتياطية من البرامج والبيانات مأخوذة على فترات متقاربة.
- الاحتفاظ بهذه النسخ في مكان آمن بعيداً عن الحاسب الآلي.
- الاحتفاظ بسرية كلمة المرور وتغييرها من وقت لآخر.
- عدم ترك البيانات معروضة على الشاشة وتغادر المكان.
- إغلاق الجهاز قبل أن تترك مكانك أمامه.
- الاحتفاظ بالرقم المتسلسل للجهاز والقرص الصلب.
- عدم القيام بتحميل أية بيانات شخصية دون التنسيق مع مسئول أمن المعلومات.
- الاتصال فوراً بمسئول مساندة المستفيدين عند ظهور أية مشكلة.
- وضع شريطة الحماية أو غلق فتحة التأمين للأقراص المرنة بعد الانتهاء من استخدامها لمنع الكتابة عليها بشكل غير مقصود.

طرق العلاج

ويقدم المهندس داود طرقاً لعلاج آثار الفيروسات وذلك على النحو التالي:

- عند اكتشاف برامج ملوثة ضمن برامج التطبيقات يجب إزالتها فوراً فإذا تم الاكتشاف في الوقت المناسب فيمكن أن تحل محلها النسخة النظيفة من البرنامج المحفوظة لدى المؤسسة، أما إذا تم اكتشافها بعد فوات الأوان فمن الضروري في هذه الحالة فحص مكتبة البرامج كلها بعناية وإزالة برامج دخيلة.
- إذا كان التخريب عن طريق حذف بعض برامج التطبيقات فعادة يكون الاحتفاظ بالنسخة الورقية للبرامج (قائمة المصدر للبرنامج) مفيداً حتى لو كانت هذه النسخة الورقية تمثل إصداراً قديماً من البرنامج فيمكن عن طريقها استعادة البرنامج المحذوف.
- بعد حدوث أي حالة تخريب يجب فحص قائمة البرامج الموجودة في الأجهزة المختلفة ومقارنتها بالقائمة السابقة على عملية التخريب لاكتشاف أي برامج دخيلة وذلك بالتأكد من أسماء البرامج وأحجامها وتاريخ آخر تعديل عليها، أما إذا كان التخريب الذي وقع في شكل تضمين كود مدسوس في بعض البرامج المشروعة فإن وسيلة اكتشاف ذلك هي استخدام برامج اختبار خاصة أو بمقارنة الكود الموجود بعد التخريب مع نسخة سابقة نظيفة.
- إذا كانت البيانات هي التي تم تخريبها فيجب في هذه الحالة فحص البيانات وإزالة أي تغييرات تكون قد طرأت عليها. فإذا كان التخريب قد تم اكتشافه في الوقت المناسب فيمكن إحلال نسخة قديمة نظيفة من البيانات محل النسخة الملوثة، ومن ثم إعادة التشغيل من النسخة القديمة ثم العمل على تحديثها.

أما إذا كان اكتشاف التخريب قد تم بعد مرور فترة طويلة وكان من الصعب العودة إلى نسخة سابقة من البيانات ففي هذه الحالة يجب طلب معونة أحد خبراء أمن البيانات لينضم لفريق العمل المكلف بمعالجة الموقف. □